CHALL 48H

WRITEUP

Cookie_Box

Etape n°1 :

On arrive sur une page de connexion nous demandant un login et un mot de passe.

En regardant le javascript en détail, on remarque qu'un cookie est créer sur le site si on ne remplit pas le formulaire et qu'un cookie fictif est créer sur une url différente.

Etape n°2 :

On remarque que pour obtenir le flag il faut que le cookie login soit égal à « admin » et que le mot de passe soit égal à « 1234 ».

Etape n°3 :

Créons donc un cookie vide et modifions sa valeur en admin. Rentrons le mot de passe ci-dessus. Le flag apparait.